UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,352	11/13/2001	Art Shelest	212159	8322

23460 7590 10/01/2004

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/010,352	**Applicant(s)** SHELEST ET AL.	
	Examiner Pramila Parthasarathy	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04/14/2003*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 04/14/2003. This application is a continuation-in-part of application 09/833,922, filled on April 12, 2001. Claims 1 – 22 were received for consideration. Preliminary amendments were filed on 04/04/2002. No Claims were cancelled. Claims 1 – 22 are currently being considered.

2. An initialed and dated copy of Applicant's IDS form 1449 is attached to the Office action.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1 - 22 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 2, 16, 18, 21 and

25 of copending Parent Application Serial Number (SN) 09/833922, hereinafter "09/833922" in view of Diffe et al. (U.S. Patent Number RE. 36,946 hereinafter "Diffie").

This is a provisional obviousness-type double patenting rejection.

A partial correspondence between the parent claims and the continuation claims are as follows:

Continuation Claim	Parent Claim
1, 2	2
4, 5, 15, 16,17	25.
12	24
7, 8, 9, 10	18
13, 19, 20	21
22	16

More specifically,

Per Claims 1, 2:

These claims recite creating authentication information and making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature which are recited in the Claim 2 of SN 09/833922. Claims 1 and 2 additionally recite sending the authentication information in a packet option. Diffie teaches sending the authentication information message in a packet option to provide both integrity and privacy of the data packets (Diffie Column 6 line 66 – Column 7 line 10). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of sending the authentication information message in a packet option on the insecure channel/public network and still keep the data packets safe from an attacker from injecting playbacks on data packets.

Per Claims 4, 5, 15, 16 and 17:

These claims recite accessing authentication information made available by a first device; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature and accepting the content data, which are recited in the parent Claim 25 of SN 09/833922. Claims 4, 5, 15, 16 and 17 additionally recite the features “caching the public key in association with the first network address”, “second computing device accessing the public key of the first device”, “removing the public key/network address from the cache” and “first network address based on a time stamp in the authentication information”. Diffie teaches, “caching the public key in association with the first network address”, “second computing device accessing the public key of the first device”, “removing the public key/network address from the cache” and “first network address based on a time stamp in the authentication information”. (Diffie Column 7 line 38 – Column 10 line 52; Column

11 lines 58 – 67; Column 12 lines 13 – 36). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of caching the public key and second computing device accessing the public key of the first device and the first network address based on a time stamp in authentication information so that the access information can be sent over an insecure channel/public network and still keep the data packets safe from an attacker from injecting playbacks on data packets and from using time expired public key.

Per Claim 12:

This claim recites accessing authentication information made available by a first device; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature and accepting the content data` which are recited in the parent Claim 24 of SN 09/833922. Claim 12 additionally recite the features "caching the public key in association with the first network address" and "appending a modifier to the public key of the first computing device before deriving a portion of the second network address". Diffie teaches, "caching the public key in association with the first network address" and "appending the modifier to the pubic key of the first computing device before deriving a portion of the second network address". (Diffie Column 7 line 38 – Column 10 line 52; Column 11 lines 58 – 67; Column 12 lines 13 – 36). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of caching the public key and then appending the public key of the first device before deriving a porting of the second network address so that access information can be sent over an insecure channel/public network and still keep the data packets safe from an attacker from injecting playbacks on data packets or the if the authentication is not valid, the key exchange messages could allow a simple denial of service type of attack.

Per Claims 7, 8, 9 and 10:

These claims recite hashing the public key; comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion; if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing, which are recited in the parent Claim 18 of SN 09/833922. Claim 7 additionally recite the features "the portion of the network address other than the node-selectable portion comprises an element in the set: "u" bit, "g" bit, a portion of a route prefix. Diffie teaches, "the portion of the network address other than the node-selectable portion comprises an element in the set: "u" bit, "g" bit, a portion of a route prefix (Diffie Column 5 line 59 – Column 6 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of including the network address from the set "u" bit, "g" bit, a route of prefix so the access information can be sent over an insecure channel/public network and still keep the data packets safe from an attacker from injecting playbacks on data.

Per Claims 13, 19 and 20:

These claims recite "accessing authentication information made available to the second computing device", "comparing the public key and network address of the first computing device with a public key/network address of the first computing device with a public key/network address association in the cache" and "accepting the content data" which are recited in the Claim 21 of SN 09/833922. Claims 13 and 19 additionally recite "determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information" and "determining whether to accept the content data based on a time stamp in the authentication information". Diffie teaches determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information and determining whether to accept the content data based on a time stamp in the authentication information (Diffie Column 3 line 45 – 52; Column 8 lines 18 – 67 and Column 12 lines 17 – 25). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of accessing the public key /network address based on a time stamp in authentication information so that the access information can be sent over the public network and still provide both integrity and privacy for the authentication information and data packets.

Claim 22:

This claim recites a data structure comprising a first data field containing data representing a public key of a computing device; and a second field containing data representing a network address of the computing device, which are recited in the Claim 16 of SN 09/833922. Claim 22 additionally recites "a third data field containing data representing a time stamp. Diffie teaches a third data field containing data representing a time stamp (Diffie Column 7 lines 7 –10). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of sending the authentication information message with a valid time stamped public key in a packet option on the insecure channel/public network the data packets safe from an attacker from injecting playbacks on data packets.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1- 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Diffie et al (U.S. Patent Number Re. 36,946).

Regarding Claims 1 and 2, Diffie teaches and describes a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45); ; and

making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the second digital signature in a packet option (Column 6 line 60 – Column 7 line 10 and Column 9 line 46 – Column 10 line 9).

Regarding Claims 3 and 5, Diffie teaches and describes a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58);

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data a hash value of data including the content data, wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded (Column 7 line 46 – Column 8 line 58 and Column 12 lines 13 – 36).

Regarding Claims 6 and 8, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

hashing the public key; comparing a porting of a value produced by the hashing with a portion of the network address other than the non-selectable portion; if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing, and if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

Regarding Claim 9 and 10, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

hashing the public key and at least a portion of the route prefix of the network address; setting the node-selectable portion of the network address to a portion of the value produced by hashing; checking to see if the network address as set is already in use; and if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

Regarding Claims 11 and 17, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58); and

cashing the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Column 7 line 38 – Column 10 line 53; Column 11 line 58 - 67 and Column 12 line 13 – 30).

Regarding Claims 18 and 20, Diffie teaches and describes a method for a computing device to use a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58);

accepting the content data if the public key and network address of the first network device match the public key/network address association in the cache (Column 5 line 59 – Column 6 line 7; Column 8 lines 18 – 67 and Column 12 lines 13 – 30).

Regarding Claim 21, Diffie teaches and describes a computer-readable medium having stored thereon a data structure of authentication information, the data structure comprising:

a first data field containing data representing a public key of a computing device; and a second data field containing data representing a network address of the computing device, the network address derived, at least in part, from a hash of the public key (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53).

Claim 4 is rejected as applied about in rejecting Claim 3. Furthermore, Diffie teaches and describes a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the second computing device accesses the public key of the first computing device over an insecure channel to a device in the set: the first computing device, a key publishing device (Column 7 38 – 55).

Claim 7 is rejected as applied about in rejecting Claim 6. Furthermore, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the portion of the address other than the node-selectable portion comprises an element in the set: “u” bit, “g” bit, a portion of a route prefix (Column 5 line 59 – Column 6 line 25).

Claim 12 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Column 7 line 41 – Column 8 line 11).

Claim 13 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information (Column 3 lines 45 – 52).

Claim 14 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

comparing the first network address against a network address in a public key/network address in a public key/network address association already in the cache; and if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then discarding the public key and the first network address without caching them (Column 7 line 38 – Column 10 line 47).

Claim 16 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

associating a timer with the caching of the public key/network address association; resetting the timer if a second public key/network address association, identical to the public key/network address association, is presented for caching; and if the timer expires, removing the public key/network address association from the cache (Column 7 line 38 – Column 10 line 47).

Claim 19 is rejected as applied about in rejecting Claim 18. Furthermore, Diffie teaches and describes a method for a computing device to use a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

determining whether to accept the content data based on a time stamp in the authentication information (Column 8 lines 18 – 67 and Column 12 lines 17 – 25).

Claim 22 is rejected as applied about in rejecting Claim 21. Furthermore, Diffie teaches and describes a computer-readable medium having stored thereon a data structure, (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

a third data field containing data representing a time stamp (Column 7 line 7 – 10).

Claim 15 is rejected as applied about in rejecting Claim 14. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache (Column 10 lines 41 – 52).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hayosh (U.S. Patent Number 6,600,823) Apparatus and Method for enhancing check security.

Atkinson (U.S. Patent Number 5,511,122) Intermediate Network Authentication

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
September 24, 2004.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100